What is claimed is:

1. An apparatus comprising:

a video camera;

a microphone;

a display;

a speaker;

an input for receiving status data;

a base unit comprising:

means for receiving the output signal of said video camera and preparing said output signal for compression;

an analog-to-digital converter coupled to convert audio signals from said microphone to digital data;

a buffer and merge circuit functioning to merge said status data with the frames of video data output by said means for receiving to generate composite live digital video data, and for buffering the resulting composite live digital video data;

a compression circuit for compressing said composite live digital video data stored in said buffer using any compression algorithm, and for compressing said audio data output by said analog-to-digital converter using any compression algorithm;

a digital video tape recorder or other removable medium recording device for recording said frames of compressed video data and said audio data;

local playback means for receiving said composite live digital video from said buffer and merge circuit and for displaying at least said video frames from said video camera along with a selected number of items of said status data on said display and for playing audio captured by said microphone on said speaker; and

means for controlling said base unit.

2. The apparatus of claim 1 further comprising an anti-tampering circuit coupled to receive said compressed frames of video data and said compressed audio data and for computing a digital signature on every frame of compressed data and for encrypting each said digital signature and recording said encrypted digital signature data on said digital video tape recorder or other removable medium recording device.

3. The apparatus of claim 1 further comprising an anti-tampering means coupled to receive compressed data and for tamper proofing said data to generate tamper proof data and recording said tamper proof data on said digital video tape recorder or other removable medium recording device.

4. The apparatus of claim 1 wherein said video camera is an analog video camera.

5. The apparatus of claim 1 wherein said video camera is a digital video camera.

6. The apparatus of claim 1 wherein said video camera is a wireless video camera, and wherein said means for receiving a signal from said video camera includes a receiver for receiving and demodulating radio frequency signals from said video camera and circuitry to develop digital video data suitable for compression from the received radio frequency signals.

7. The apparatus of claim 1 wherein said microphone is a wireless microphone and said base unit includes a receiver to receive and demodulate radio frequency signals from said wireless microphone to develop an audio signal and apply the audio signal to said analog-to-digital converter

8. An apparatus comprising:

a video camera;

a microphone;

a display;

a speaker;

an input for receiving status data;

a base unit comprising:

means for receiving the output signal of said video camera and preparing said output signal for compression;

an analog-to-digital converter coupled to convert audio signals from said microphone to digital data;

a buffer and merge circuit functioning to merge said status data with the frames of video data output by said means for receiving to generate composite live digital video data, and for buffering the resulting composite live digital video data and for detecting sync intervals in said frames of video data output by said means for receiving and outputting a frame signal, and for receiving at least frame number data that increments with each received frame and merging said frame number data into said composite live digital video data stream;

a compression circuit for compressing said composite live digital video data stored in said buffer using any compression algorithm, and for compressing said audio data output by said analog-to-digital converter using any compression algorithm;

anti-tampering means for receiving said compressed video and audio data and rendering it tamper proof;

a digital video tape recorder or other removable medium recording device for recording whatever data is output by said anti-tampering means;

local playback means for receiving said composite live digital video from said buffer and merge circuit and for displaying at least said video frames from said video camera along with a selected number of items of said status data on said display and for playing audio captured by said microphone on said speaker; and

means for controlling said base unit including a frame counter for receiving said frame signal and for incrementing a frame count each time said frame signal is received and for supplying said frame count data as status data to said buffer and merge circuit.

9. The apparatus of claim 8 wherein said video camera is an analog video camera.

10. The apparatus of claim 8 wherein said video camera is a digital video camera.

11. The apparatus of claim 8 wherein said video camera is a wireless video camera, and wherein said means for receiving a signal from said video camera includes a receiver for receiving and demodulating radio frequency signals from said video camera and circuitry to develop digital video data suitable for compression from the received radio frequency signals.

12. The apparatus of claim 8 wherein said system controller also includes a clock and supplies time of day data to said buffer and merge circuit as status data, and wherein said buffer and merge circuit functions to merge said time of day data into said composite live video data stream.

13. The apparatus of claim 8 wherein means for local playback is controlled by said means for controlling as to which items of said status data are overlaid on the displayed video and wherein said means for local playback further comprises an input for receiving compressed video and audio data and said status data recorded on said digital video tape recorder and functions to decompress said video and audio data and display the decompressed video data along with zero or more items of selected status data on said display and convert said decompressed audio data to an audio signal and play it on said speaker.

14. The apparatus of claim 8 wherein means for local playback is controlled by said means for controlling as to which items of said status data are overlaid on the displayed video and wherein said means for local playback further comprises an input for receiving compressed video and audio data and said status data recorded on said digital video tape recorder and functions to decompress said video and audio data and display the decompressed video data along with zero or more items of selected status data on said display and convert said decompressed audio data to an audio signal and play it on said speaker.

15. The apparatus of claim 8 wherein said microphone is a wireless microphone and said base unit includes a receiver to receive and demodulate radio frequency signals from said wireless microphone to develop an audio signal and apply the audio signal to said analog-to-digital converter

16. An apparatus comprising:

a video camera;

a microphone;

a display;

a speaker;

an input for receiving status data;

a base unit comprising:

means for receiving the output signal of said video camera and preparing said output signal for compression;

an analog-to-digital converter coupled to convert audio signals from said microphone to digital data;

a buffer and merge circuit functioning to merge said status data with the frames of video data output by said means for receiving to generate composite live digital video data, and for buffering the resulting composite live digital video data, and for recognizing a sync signal in the incoming video data and outputting a frame signal, and for receiving a frame count signal and merging said frame count as status data in said composite live digital video data;

a compression circuit for compressing said composite live digital video data stored in said buffer using any compression algorithm to generate compressed composite live digital video data, and for compressing said audio data output by said analog-to-digital converter using any compression algorithm to generate compressed audio data;

a hard disk means for receiving and continuously recording said compressed composite live digital video data along with said compressed audio data, and for receiving an archive signal

commanding playback of recorded data and specifying in any way at least the starting point in the stream recorded data where said playback is to begin;

a digital video tape recorder or other removable medium digital data recording device for recording compressed data output by said hard disk means when a record signal is received; and

control means for controlling said base unit and including at least a frame counter, said control means also coupled to receive said frame signal and for incrementing said frame counter each time said frame signal is received and for supplying said frame count to said buffer and merge circuit as status data.

17. The apparatus of claim 16 further comprising anti-tampering means coupled to receive said compressed data output by said compression means and rendering said compressed data tamper proof.

18. The apparatus of claim 16 further comprising local playback means for receiving said live digital video from said buffer and merge circuit and for displaying at least said video frames from said video camera along with a selected number of items of said status data on said display and for playing audio captured by said microphone on said speaker.

19. The apparatus of claim 16 further comprising local playback means for receiving said live digital video from said buffer and merge circuit and recorded, compressed video, status and audio data from said hard disk means or said digital video tape recorder and for selection of one source of video, status and audio data under control of said control means and for decompressing at least the selected compressed video and audio data and for displaying the decompressed video along with a selected number from zero to some larger number of items of said status data on said display and for playing audio captured by said microphone on said speaker.

20. An apparatus comprising:

one or more video inputs, each for receiving either an analog or a digital video signal and outputting a video signal;

zero or more wireless video input means for receiving either an analog or a digital video signal that is transmitted by electromagnetic transmission and for outputting a zero or more video signals;

means for selecting a video signal from any of said one or more video inputs or said zero or more wireless video inputs and appropriately preparing said video signal as digital data ready for compression, the type of preparation being dependent upon whether the video signal selected is digital or analog;

one or more audio inputs for receiving audio signals and outputting same;

zero or more wireless audio input means for receiving audio signals modulated onto an electromagnetic carrier and outputting zero or more audio signals;

means for digitizing the audio signals output by said one or more audio inputs and said zero or more wireless auido input means to generate one or more channels of digital audio data;

zero or more data paths for receiving one or more types of system status data including a time of day signal and/or a frame counter signal;

a buffer and merge circuit for receiving the digital data of the selected video signal and said status data and merging them into a live digital video stream of data which includes said status data;

compression means for receiving said live digital video stream of data and said one or more channels of digital audio data and for compressing all said data using any compression algorithm;

anti-tamper means for receiving compressed data output by said compression means and rendering it tamper proof;

a hard disk for continuously recording the compressed data output by said compression means;

a digital video cassette recorder or other removable medium digital data recording means for recording digital data, coupled to said anti-tamper means and said hard disk, for recording digital data;

controller means for receiving operator input and for controlling which video signal input is selected and which microphone input is selected and controlling said

recorder means to record data directly from said anti-tamper means or data played back from said hard disk or to not record data at all and for controlling said hard disk to search for and playback data starting from a starting point designated by an operator, which can be a previously recorded time or frame, and for controlling said recorder means to record said played back data from said hard disk to provide an after-the-fact recording capability; and

playback means for providing outputs from which a video image may be derived and sound waves may be generated, said playback means having as a video and audio input either said live digital video stream of data and live audio data or previously recorded compressed video and audio data, the source of video and audio data being under control of said controller means, and providing video data and audio signals for playback thereby providing the ability to display and hear live video and audio or previously recorded video and audio.

21. A process to tamper proof digital data absent a conspiracy between more than one person holding key pairs, comprising the steps:

(1) generating digital data of any type that is to be rendered tamper proof;

(2) assigning each of a plurality of multiple encryption/decryption key pairs to a different person;

(3) calculating one or more digital signatures on the data to be protected;

(4) encrypting the encryption key of a first key pair belonging to a first person to be used to encrypt said digital signature data using the encryption key of a second key pair;

(5) having a second person temporarily supply the decryption key of said second key pair and using it to decrypt said encryption key of said first key pair and store said encryption key of said first key pair in volatile memory in the clear;

(6) monitoring for the occurrence of any physical or electrical phenomenon or event which would indicate the possibility that said digital data to be protected has been accessed improperly or tampered with;

(7) determining if said phenomenon or event has occurred indicating improper access or possible tampering;

(8) if so, erasing said encryption key of said first key pair and performing any suitable anti-tampering protocol such as blocking all access to said data to be protected, blocking all recording of said data to be protected or placing a notation in said data that it may have been tampered with or accessed improperly;

(9) if said phenomenon or event indicating improper access or possible tampering has not occurred, encrypting said digital signature data using said encryption key of said first key pair which is stored in the clear in said volatile memory and then encrypting these results with the encryption key of a third key pair.

22. The process of claim 21 further comprising the steps of recording the encrypted signature data and said data to be protected and a step for verifying that said recorded data has not been tampered with by comparison of digital signatures.

23. The process of claim 21 wherein said encryption of step 9 is of the digital data to be protected itself and not encryption of digital signature data calculated from the data to be protected, and wherein step (3) is eliminated.

24. A process to tamper proof digital data absent a conspiracy between more than one person holding key pairs, comprising the steps:

(1) generating digital data of any type that is to be rendered tamper proof;

(2) assigning each of a plurality of multiple encryption/decryption key pairs to a different person;

(3) calculating one or more digital signatures on the data to be protected;

(4) encrypting the encryption key of a first key pair belonging to a first person to be used to encrypt said digital signature data using the encryption key of a third key pair assigned to a third person and then encrypting that result with the encryption key of a second key pair assigned to a second person and storing the double encrypted result in volatile RAM;

(5) having said second person temporarily supply the decryption key of said second key pair and using it to decrypt said double encrypted result to generate a single encrypted result and store said single encrypted result in volatile memory;

(6) having said third person temporarily supply the decryption key of said third key pair and using it to decrypt said single encrypted result to generate an in-the-clear version of the encryption key of said first key pair, and storing same in volatile RAM;

(7) monitoring for the occurrence of any physical or electrical phenomenon or event which would indicate the possibility that said digital data to be protected has been accessed improperly or tampered with;

(8) determining if said phenomenon or event has occurred indicating improper access or possible tampering;

(9) if so, erasing said encryption key of said first key pair from said volatile memory and performing any suitable anti-tampering protocol such as blocking all access to said data to be protected, blocking all recording of said data to be protected or placing a notation in said data that it may have been tampered with or accessed improperly;

(10) if said phenomenon or event indicating improper access or possible tampering has not occurred, encrypting said digital signature data using said encryption key of said first key pair which is stored in the clear in said volatile memory.

25. The process of claim 24 further comprising a step for verifying the integrity of said data to be protected by comparison of digital signatures.

26. The process of claim 24 wherein step (3) is eliminated and wherein step (10) comprises encrypting the data to be protected itself using the encryption key of said first key pair instead of digital signature data computed therefrom.

27. A process to tamper proof digital data absent a conspiracy between more than one person holding key pairs, comprising the steps:

(1) generating digital data of any type that is to be rendered tamper proof;

(2) assigning each of a plurality of multiple encryption/decryption key pairs to a different person;

(3) calculating one or more digital signatures on the data to be protected;

(4) storing the encryption key of a first key pair belonging to a first person to be used to encrypt said digital signature data in nonvolatile RAM;

(5) having said second person temporarily supply the encryption key of said second key pair and storing it in volatile memory;

(6) having a third person temporarily supply the encryption key of said third key pair;

(7) monitoring for the occurrence of any physical or electrical phenomenon or event which would indicate the possibility that said digital data to be protected has been accessed improperly or tampered with;

(8) determining if said phenomenon or event has occurred indicating improper access or possible tampering;

(9) if so, erasing said encryption key of said second key pair and/or said third key pair from said volatile memory and performing any suitable anti-tampering protocol such as blocking all access to said data to be protected, blocking all recording of said data to be protected or placing a notation in said data that it may have been tampered with or accessed improperly;

(10) if said phenomenon or event indicating improper access or possible tampering has not occurred, encrypting said digital signature data using said encryption key of said first key pair and then encrypting that result using said encryption key of said second key pair, and then encrypting that result using said encryption key of said third key pair.

28. The process of claim 27 further comprising a step for verifying the integrity of said data to be protected by comparing digital signature data.

29. The process of claim 27 wherein step (3) is eliminated and step (10 comprises encrypting the actual data to be protected instead of digital signature data calculated therefrom using the encryption keys of said first, second and third key pairs.